GÖTEBORGS UNIVERSITET

Molnet,
upplevda kontra faktiska risker
- vägen till ökad medvetenhet.

The Cloud
Perceived versus actual risks, the path to greater awareness.

Teysir Hassan

Kandidatuppsats i informatik

Rapport nr. 2011:006
ISSN: 1651-4769

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2011

Abstrakt

Molnets framsteg har varit oundvikliga de senaste åren. Det finns emellertid fortfarande många osäkerheter rörande molnet och molntjänster främst i områden rörande risker inom datasäkerhet, juridik samt organisationen. För att undersöka upplevda respektive faktiska risker utfördes en undersökning. Undersökningen formades från ett besök på ett företagsseminarium utfört av ett konsultföretag i Göteborg som berörde kravställning i molnet. Undersökningen bestod av intervjuer med konsulter på samma företag, med fokus på molnet och deras kunders upplevda oro kring risker med molnet. Svar söktes med stöd från litteratur på tidigare nämnda områden. Oron samt de främsta riskerna rörde sig kring oklarheterna i molnleverantörsavtal, sekretess och åtkomstbehörigheter samt frågor gällande lagar och regelverk.

Även om det fanns många oklarheter samt svårigheter rörande de legala aspekterna, visade det sig vara en större upplevd risk än faktiskt risk.

Nyckelord:
Molnet, molntjänster, medvetenhet, risker

Abstract

The progress in Cloud Computing has been inevitable the past few years. However, there are still many uncertainties concerning Cloud Computing services primarily in areas related to risks in data security, legislation and organization. To investigate the perceived and actual risks, a study was conducted. The study was formed from a visit to a business seminar conducted by a consulting company in Gothenburg that concerned requirements definition in the Cloud. The study consisted of interviews with consultants on the same company, with a focus on the cloud and their customers' concerns about perceived risks in the Cloud. Answers were sought with the support of literature on the aforementioned areas. The concern and the main risks were about lack of clarity of cloud vendor contracts, confidentiality and access privileges, and issues relating, laws and regulations.

Although there were several uncertainties and difficulties concerning the legal aspects, it appeared to be a more perceived risk than actual risk.

Keywords:
The cloud, cloud computing, awareness, risks

Förord

Vill börja med att tacka min handledare Ted Saarikko som har handlett mig i utformningen av uppsatsen samt i mitt arbete.

Ett stort tack vill jag även ge till Acando i Göteborg för möjligheten att utföra studien hos er. Speciellt tack till Martin Ström och Johan Hedlund som har stöttat mig i arbetet samt med stort tålamod svarat på mina frågor och funderingar.

Jag vill även tacka alla respondenter på Acando som ställde upp för intervjuerna.

Till sist vill jag tacka min fästmö som varje dag varit vid min sida och stöttat mig.

Göteborg, 23 maj, 2011

Teysir Hassan

Innehållsförteckning

1. Introduktion

Traditionellt sett är det lätt att bli bekväm i hur det alltid har varit och fungerat. Tryggheten skapar en försiktighet vilket ger en tendens att det förblir traditionellt. När ny teknik möjliggör nya sätt att leverera samt använda IT står man i bästa fall inför ett paradigmskifte. Ett paradigmskifte, vilket i många traditionella aktörers ögon innebär en ny oro för det nya samt okända. Nytt område, nya risker.

Molnet är det ”nya området”. Det betyder emellertid inte att allt nytt endast för med sig risker. Det finns nya möjligheter likaså. Möjligheter som oftast övervinner riskerna. Användning av molnet har visat sig vara en möjliggörare som bland annat kostnadsbesparare eftersom man slipper själv investera i hårdvara och kompetens. När företag istället låter en molnleverantör förvalta infrastrukturen som används kan man istället fokusera på det som verkligen är viktigt, företagets kärnverksamhet.

Vidare så har hög flexibilitet i molntjänster även gett möjligheten att kunna på ett effektivare sätt svara på marknaden. Överlag har stora företag alltid haft dominans på marknaden. Däremot med molntjänstens framsteg har, i den meningen att man låter någon annan sköta infrastrukturen, har även mindre företag fått chansen att kunna konkurrera med de stora.

1.1 Bakgrund

Den senaste tiden har det varit svårt att ha undgått molnet och molntjänster. Cloud computing som är engelskan motsvarighet, har diskuterats flitigt i media och var en stor nyhet runt 2009-10, likaså diskuterades molntjänster vara, ”det nästa stora”. Man hade väldigt höga tankar om molnet som fenomen och påverkade synen kring IT som vi tidigare sett den. Eftersom uppståndelsen runt molnet kom så plötsligt och växte så snabbt fann många att osäkerheten kring molnet var stor. Ännu idag har molntjänster inte riktigt lyckats ta över(Glaad, 2011).

Enligt Gartners ”Hype Cycle” (Smith, 2010) har molnet under 2010 precis kommit över toppen på kurvan av höga förväntningar och hädanefter förväntas molnet bli allt mer konventionell, den processen kommer emellertid pågå under flera år framåt(ibid.).

I en intervju med Per Adolfsson, VD för Microsoft i Sverige, nämner han att molnet kommer att växa kraftigt under 2011(Rosengren, 2011). Men än idag finns det många beslutsfattare inom företag som känner stor osäkerhet för molnet och förstår inte riktigt vad molntjänster kan innebär för den egna verksamheten(Rådmark, 2011a).

Med molntjänster finns det möjlighet att flytta ut allt på webben och begränsningarna kring hur och var man arbetar minskar. Det enda man behöver är en Internetuppkoppling och en webbläsare. Det man oftast inte tänker på är att i den publika webben har man redan använt molnet i stor utsträckning till exempel som e-post (Conway, 2011).

För företagen och deras system har det däremot varit annorlunda. Ett företag har inte lika stor frihet som en privatperson när det gäller lagar och regelverk man måste ta

hänsyn till. Emellertid är möjligheterna lika stora och molntjänster har uppfattats som väldigt lovande för företag om man tänker på möjligheterna den ger, däremot med allting tillkommer alltid en risk. I en rapport från Gartner skriver de att oron för risken ofta upplevs mer än vad som behövs. Gartner skriver;

> *"Many IT organizations encounter resistance from legal, compliance or risk managers when considering cloud computing for personal information. Security and privacy concerns are currently the most visible inhibitors to cloud computing. […] This will change when organizations decide that some of these concerns are without basis and that the remaining risks can be mitigated or accepted."* (Casper, 2011 s.1)

1.2 Syfte och frågeställning

Mitt syfte med denna studie är först och främst öka kunskapen samt öka medvetenheten hos företag kring molnet samt att undersöka vad det finns för upplevda risker respektive faktiska risker med att placera tjänster och information i molnet. Genom att öka medvetenheten kring riskerna samt vara mer förberedd kan man i förlängningen bli mer tryggare i sina beslut vid köp samt införande av molntjänster.

Frågeställningen för denna uppsats blir följaktligen:

- Vad finns det för risker med att placera tjänster och information i molnet?

1.3 Avgränsningar

Med risker kan man knyta an flera aspekter med och en risk kan uppfattas olika beroende på person. I denna uppsats har jag valt att avgränsa mig till ett företagsseminarium jag besökte. Områden som berördes av deltagarna under seminariet var bland annat risker gällande datasäkerhet, legala aspekter och organisatoriska aspekter.

Har emellertid valt att utelämna de ekonomiska aspekterna molnet medför eftersom det är konstaterat i artiklar och undersökningar att användning av molntjänster möjliggör kostnadsbesparingar. Bland annat visar en artikel i CIO Sweden att enbart i Europa kommer företag under 2011 spara uppemot 700miljarder kronor på att använda molntjänster(Rådmark, 2011b).

2. Metod

Studien har till stor del utformats från ett seminarium jag fick möjligheten att besöka. Seminariet ägde rum i Göteborg och utfördes av konsultföretaget Acando. Seminariet som var ämnat för företag var en introduktion till molntjänster och hur dessa kunde vara en tillgång för verksamheten. Med ett rum fullsatt med nyfikna beslutsfattare, handlade större delen utav frågorna som ställdes om just datasäkerheten och risker med att lägga ut företagsdata ut i molnet. Det framstod att viljan fanns och intresset uppfattades som starkt för molnet och molntjänster. Det uppfattades emellertid som att beslutsfattarna ändå ville var försiktiga men osäkerheten gav fortfarande upphov till att man tog ett steg tillbaka och väntade med att gå över till molnet. Som Monica Claeson, molnexpert på IBM, nämner i en intervju att innan man beslutar om en molntjänst är det a och o att säkerställa ur ett säkerhetsperspektiv hur informationen behandlas av molntjänsteleverantörerna (Cooke, 2011).

Observationerna gjordes under seminariet och frågor som uppkom antecknades flitigt. För att få en ytterligare förförståelse över problematiken innan undersökningen, genomfördes även en mindre litteraturstudie som tillsammans med seminariet låg till grund för utformningen av den empiriska studien. Intervjufrågorna utarbetades utifrån berörda områden från seminariet samt med stöd från litteraturen.

2.1 Vetenskaplig ansats

Det vetenskapliga förhållningssättet fenomenografi i den empirinära ansatsen har tillämpats för denna studie (Patel & Davidson, 2003). I fenomenografin är fokuset riktat mot att studera uppfattningar(ibid.). Syftet med en fenomenografisk analys är att studera hur fenomen i omvärlden uppfattas av människor(ibid.). Fenomenet som ska studeras i detta fall blir, hur risker i molnet samt molntjänster uppfattas.

När man utför en studie arbetar man inte endast med teori utan även att få så korrekt kunskap om verkligheten som möjligt. Kunskapen om verkligheten man har samlat in kallas för ”empiri”(Patel & Davidson, 2003). För att kunna relatera teorin med empirin finns det huvudsakligen tre stycken alternativ sätt; deduktion, induktion samt abduktion(ibid.). Genom att arbeta *deduktivt* innebär att man från befintliga teorier drar slutsatser för att sen prövas i empirin, verkligheten(ibid.). Att arbeta på ett *induktivt* sätt innebär istället att man från empirin utformar en teori(ibid.). Sista alternativet att relatera teori med empiri är genom abduktion. Man kan säga att abduktion är en hybrid mellan deduktion och induktion. I ett abduktivt arbetssätt börjar man med att från en empiri utforma en teori(induktion) vilket därefter utvecklas samt prövas ytterligare i empirin(deduktion) för att kunna utforma en ny teori(ibid.).

I den här studien har ett abduktivt arbetssätt tillämpats.

2.2 Litteraturstudie

För sökning av litteratur började jag med att söka på begreppet ”molnet” och ”molntjänster” på svenska och engelskans motsvarighet ”Cloud Computing”, på Göteborgs Universitetsbibliotekets hemsida (ub.gu.se). Sökte bland annat i GUNDA, GUPEA samt de samtliga artikeldatabaser man får tillgång till. Sökte även genom Chalmers biblioteks Chans i artikeldatabaser. Använde mig även utav Google Scholar vid sökning av artiklar, likaså sökte jag efter rapporter från Gartner. Genom detta fick jag en överblick på uppsatser/artiklar/rapporter som hittills skrivits och vilka arbeten möjligtvis kan vara relaterat till den frågeställning jag valt att undersöka.

På ub.gu.se sökte jag igenom samtliga databaser efter artiklar samt böcker med begrepp rörande molnet samt molntjänster som dök på seminariet översatt till engelska; ”Cloud Computing” följt av något följande ord som bland annat; ”definition”, ”risks”, ”risk assessment”, ”legal issues”, ”security”, ”privacy”.

I GUPEA befann sig väldigt få examensarbeten kring molnet, de examensarbeten som varit intressanta för frågeställningen har jag undersökt referenserna för att se om även de kan vara till hjälp för mig för att kunna besvara frågeställningen.

Jag har även sökt igenom analyser och rapporter från Gartner som behandlar ämnet kring molnet och en utav den senaste rapporten har de undersökt hur så pass stor oro det finns bland företagen för den personliga integriteten och att lägga ut företagsdata i molnet(Casper, 2011). Annat material från Gartner bland annat som ovannämnda rapport har varit till stor hjälp för att kunna svara på frågeställningen.

Som stöd har jag även läst igenom tidningsartiklar publicerade på Internet, från bland annat ”CIO Sweden”, ”Cloud Magazine” och ”Computer Sweden”, rörande frågor kring molnet. Detta för att få så färsk och relevant information kring ämnet som möjligt. De artiklarna som jag refererat till i tidigare kapitel har visat på att undersöknings-problemet är till högsta grad aktuellt.

2.3 Intervjuer

Patel & Davidson(2003) menar att innan man utför en intervju måste man informera respondenten om syftet för intervjun samt klargöra hur respondentens bidrag kommer att användas. Vidare måste man även klargöra om intervjun är konfidentiell eller inte(ibid.). Patel & Davidson (2003) menar vidare att respondenter ofta blir utvalda utan det egna initiativet, vilket kan medföra att respondenten inte ser någon nytta med att besvara frågorna. Därför, innan intervjuerna tog plats, skickades en introduktion till samtliga respondenter med bakgrundsinformation, syfte för intervjun, varför respondentens bidrag är viktigt samt hur materialet kommer att användas. Respondenterna fick vara anonyma och materialet behandlades konfidentiellt.

Valda metoden för intervjuer var den kvalitativa ansatsen med semi-strukturerade frågor. Enligt Patel & Davidson(2003) används kvalitativa intervjuer för att upptäcka

samt identifiera egenskaper och beskaffenheten hos/i något. I den här studiens fall, respondentens uppfattning om molnet samt molntjänster.

2.3.1 Introduktion till Acando

Acando är ett svenskt konsultföretag inom IT och Management som tillsammans med kunderna identifierar och genomför verksamhetsförbättringar med hjälp av informationsteknik. Den svenska verksamheten är indelad i följande affärsområden:

- Management Consulting
- Strategic IT
- SAP
- Microsoft Dynamics
- IT Solutions
- Business Intelligence

Acando är även verksam i fem andra länder; Norge, Finland, Danmark, Storbritannien och Tyskland. Hela Acando koncernen har cirka 1100 medarbetare. I Sverige finns kontor i Göteborg, Stockholm, Malmö, Linköping, Västerås, Ludvika och Borlänge med totalt 640 medarbetare.

Denna studie är utförd samt hänvisar endast till kontoret i Göteborg.

2.3.2 Respondenter

Inför val av respondenter formulerades en målgrupp, vilket i sitt arbete befinner sig nära kunden samt har erfarenhet utav att ha arbetat med frågor rörande molnet. Min kontaktperson på Acando hjälpte till vid val av respondenter och bokning. Här nedan följer en presentation av respondenterna som intervjuades.

Respondent A
Arbetar med Information Management och Business Intelligence. Arbetar även som rådgivare i olika frågor vad gäller användning av IT och IT i teknik. Respondenten har flera års erfarenhet inom mjukvaruutveckling samt systemutveckling. Sen ett par år tillbaka har respondenten arbetat med frågor rörande molntjänster och dess möjligheter.

Respondent B
Arbetar som lösningsarkitekt inom Microsoft plattformen. I projekt har respondenten oftast en ledande roll samt brukar respondenten vara ansvarig för design och ser till att leveransen kommer på plats enligt önskemål. Respondenten har flera års erfarenhet inom programmering och systemutveckling, främst inom Microsoft plattformen. Respondenten arbetar med frågor rörande molnet samt praktisk erfarenhet av arbete i molnmiljö.

Respondent C
Har roll som affärsområdesansvarig för Microsoft-området. Har även i vissa fall rollen som avtalspartner i affärer med kunden. Respondenten har flera års erfarenhet av

systemutveckling främst inom Microsoft plattformen samt mångårig erfarenhet som konsultchef. Respondenten arbetar med frågor rörande molnet dock begränsad praktisk erfarenhet.

Respondent D
Har roll som ansvarig för Sharepoint-området. Har även roll som projektledare i Sharepoint-projekt. Respondenten har flera års erfarenhet som IT-konsult samt arbetar mycket med frågor rörande Enterprise 2.0. Respondenten har kommit i kontakt med frågor rörande molnet dock ingen praktisk erfarenhet.

Respondent E
Arbetar inom Java-gruppen och som bland annat har arbetat med teknisk arkitektur. Är även ansvarig för Acandos open source-satsning. Respondenten har flera års erfarenhet inom webbutveckling och programmering och mångårig erfarenhet som konsult. Respondenten arbetar med frågor rörande molnet samt praktisk erfarenhet av arbete i molnmiljö.

2.3.3 Praktiskt tillvägagångsätt

Eftersom tiden var begränsad för studien och sedan tidigare sökt kontakt med Acando samt mitt deltagande i seminariet, valde jag att intervjua konsulter på Acando istället för att intervjua individer i olika företag vars intresse är stort för molnet och molntjänster. Konsulterna på Acando som är praktiker inom molnområdet innehar en stor expertis på området samt praktiskt erfarenhet med att ha arbetat frågor rörande molnet tillsammans med kunderna.

Intervjuerna ägde rum på Acandos kontor i Göteborg. Intervjuerna utfördes under en dag. Intervjuerna tog 20-50 minuter. Längden på intervjuerna varierade beroende på hur mycket erfarenhet respondenterna hade från att i projekt med kunder praktiskt arbetat med molnfrågor.

Frågorna var uppdelade i 5 delar. Första delen började med inledande frågor om respondentens roll på konsultföretaget och respondentens bakgrund. Andra delen fortsatte med en inledande frågor kring molnet för att få en uppfattning hur respondenten resonerar kring molnet. Tredje delen fokuserade på konsultföretagets kunder hur de i sin tur resonerar kring molnet och kundernas upplevda oro. Fjärde delen var ett tillägg med mer juridikspecificerade frågor, frågor kring de legala aspekterna. Femte och sista delen var avslutande frågor kring synen på molnets framtid samt eventuella kompletteringar.

Samtliga intervjuer spelades in efter att ha frågat om tillåtelse. Intervjuerna transkriberades samt analyserades och kategoriserades enligt de områden intervjufrågorna var byggda på.

2.4 Analys av data

Det insamlade materialet kommer att analyseras samt kategoriseras i de områden intervjufrågorna är utformade ifrån. Underlag för intervjufrågorna kommer från förstudien som gjordes, de berörda områdena är följande; Hur molnet uppfattas av konsulterna, hur kunderna uppfattar molnet, hur legala aspekter uppfattas samt framtidssynen för molnet. Samtliga områden har även efter analys delats in i underkategorier för att skapa en mer hanterbar helhet dessutom kommer det insamlade materialet redovisas i form av citat med respondenternas egna ord samt anknytande text för att skapa en mer lättförstådd helhet.

2.5 Validitet och Reliabilitet

När det gäller den insamlade empirin, presenteras den genom respondenternas egna ord där man får en klarare bild av hur respondenterna uppfattar molnet samt övriga artefakter rörande frågeställningen. För att öka resultatets trovärdighet brukar man nämna kommunikativ validitet som ett begrepp (Patel & Davidson, 2003). Kommunikativ validitet innebär att de tolkningar man presenterar bör byggas så att läsaren av en forskningsrapport kan bilda en egen uppfattning(ibid.). För studier som bygger på intervjuer kan man öka den kommunikativa validiteten genom att inte rycka ut svaren ur sitt sammanhang(ibid.), därför har jag valt att redovisa respondenternas svar i längre sekvenser.

Förstudien bygger även på verklig aktuell problematik kring studiens område. Samt att en stor del utav litteraturen som använts kommer från tidningsartiklar samt Gartners forskningsrapporter rörande aktuella frågeställningar kring studiens område.

3. Teori

För att kunna svara på frågeställningen behöver man först och främst öka kunskapen om molnet. Kommer därför först att ge en introduktion till molnet samt hur det definieras och vad molnet och molntjänster innebär enligt den skrivna litteraturen.

3.1 Molnet – grundläggande kunskaper

För att generellt sätt redogöra vad molnet och molntjänster är kan med enkelhet säga att det är tjänster distribuerade via Internet. Det har emellertid visat sig inte vara lika enkelt att förklara molnet. Det har hittills varit väldigt många olika organ som har försökt sig på att definiera molnet. Här nedan följer två av de mest accepterade definitioner utav molnet. Gartner har bland annat formulerat definitionen:

> *"Cloud Computing is a style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies."* (Plummer et al. 2009. s.2)

En annan definition på molnet och molntjänster som likt Gartners, är generellt accepterad kommer från NIST(National Institute of Standards and Technology). Den lyder:

> *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resoruces (e.g. networks, servers, storage, applications and services) that can rapidly provisioned and released with minimal management effort or service provider interaction."*

I en rapport från Gartner skriver de att den egna definitionen och definitionen NIST har bidragit med är mer lik än olik, största skillnaden sägs vara terminologin (Smith & Cearley, 2010). Både Gartner och NIST har försökt att genom definitionerna klargöra på ett så simpelt sätt som möjligt, förklaringen av molntjänster. Gartner har visserligen definierat fler lager än NIST men Gartner betonar att de ytterligare lager fortfarande är lika användbara. Gartners definition ökar detaljnivån och sägs vara kompletterande till definitionen från NIST(ibid.). För att behålla simpelheten har jag emellertid valt att fokusera på definitionen från NIST.

NIST har identifierat tre stycken aspekter för molnet för att hjälpa definiera och kategorisera det(Blount & Zanella, 2010).

- Grundläggande egenskaper
- Tjänstemodeller
- Distributionsmodeller

Grundläggande egenskaper
NIST har definierat fem stycken grundläggande egenskaper som utgör en molntjänst:

1. *On-demand self-service*
   Innebär att en användare kan på egen hand, efter behov bestämma exempelvis lagring och server tid utan att behöva söka kontakt med molnleverantören (Blount & Zanella, 2010).

2. *Broad network access*
   Innebär att funktioner som finns tillgängliga via Internet, nås via standardiserade system som främjar användningen av heterogena tunna eller tjocka klientplattformar(Blount & Zanella, 2010).

3. *Resource pooling*
   Innebär att molnleverantörernas resurser är samlade för att fler användare ska kunna ta del av resurserna vi användning av en tjänst. Resurser tilldelas dynamiskt enligt användarens efterfrågan(Blount & Zanella, 2010).

4. *Rapid elasticity*
   Innebär att kapaciteten kan snabbt och elastiskt tilldelas för att vid behov, snabbt kunna skalas ut eller skalas in. I vissa fall kan detta ske per automatik(Blount & Zanella, 2010).

5. *Measured service*
   Innebär att molnsystemen automatiskt kan styra och optimera resurs-användningen genom att mäta kapaciteten vid vissa nivåer för en specifik tjänst(Blount & Zanella, 2010).

3.1.1 Tjänstemodeller

När det handlar om molnet och dess tjänster finns det ett flertal alternativ att ta hänsyn till. Det första man bör fråga sig själv är **vad** man ska flytta till molnet och det andra är **när** man ska flytta det (Blount & Zanella, 2010). När det handlar om vad så kan man flytta sin 1) infrastruktur, 2) sin mjukvaruplattform, 3) sina applikationer, 4) sin data eller en kombination av dessa. Här nedan nämns de tre huvudsakliga tjänstemodeller:

IaaS (Infrastructure as a Service)

IaaS-tjänster ger möjligheten att använda en färdig infrastruktur utan att själv behöva husera servrar i företaget. Man slipper investera pengar i hårdvara och kompetens. Eftersom det är huvudsakligen är lagring och datorkraft man hyr så kan en användare av en IaaS-tjänst till stor del själv välja vad för typ av operativsystem som ska användas. Man har även kontroll över vilka applikationer man använder (Blount & Zanella, 2010).

PaaS (Platform as a Service)

I PaaS-tjänster ingår det en infrastruktur och operativsystem. Användaren har ingen kontroll av de underliggande komponenterna emellertid har man delvis kontroll över vad för applikationer man ska använda (Blount & Zanella, 2010).

SaaS (Software as a Service)

SaaS-tjänster är den mest kända och mest använda modellen. Det enda man behöver för att använda en SaaS-tjänst är en webbläsare. Leverantören förvaltar och kontrollerar den underliggande infrastrukturen, nätverk, servrar, operativsystem, lagring och till och med funktionaliteten i applikationen. Användaren har således ingen kontroll (Blount & Zanella, 2010).

3.1.2 Distributionsmodeller

De ovannämnda tjänstemodellerna kan distribueras på olika sätt. Det finns fyra stycken huvudsakliga distributionsmodeller. Vilken modell man använder beror dels på företagets risknivå, vad man har för sekretesskrav och den egna kostnadsflexibiliteten (Blount & Zanella, 2010).

Public Cloud

I publika moln delas infrastrukturen mellan alla användare eller mellan en större branschgrupp. Om man som företag har höga krav gällande sekretess samt säkerhet finner man således inte publika moln vara tilltalande (Blount & Zanella, 2010).

Private Cloud

Privata moln passar däremot ovannämnda företag mer, med höga sekretess- och säkerhetskrav då privata moln endast drivs för en användare (Blount & Zanella, 2010). Användning av privata moln minskar säkerhetsriskerna samt obehörig dataåtkomst då ”molnägaren” har full kontroll över infrastrukturen (Conway, 2011).

Community Cloud

I denna modell, likt publika moln delar man infrastrukturen. Däremot så är den begränsad endast till valda användare. Det kan bland annat vara ett flertal företag som i gemenskap till varandra delar till exempel uppdrag eller lika krav gällande säkerhet (Blount & Zanella, 2010). Till skillnad från publika moln delas infrastrukturen mellan färre användare vilket medför i sin tur att kostnaden per användare ökar (Conway, 2011).

Hybrid Cloud

Hybrida moln kombinerar två eller flera distributionsmodeller. Exempelvis kan det vara en kombination av publika och privata moln. Där fallet kan vara att stärka upp ett privat moln med resurserna hos ett publikt moln för att exempelvis kunna hantera en plötslig ökning i arbetsbördan (Blount & Zanella, 2010).

3.2 Risker

När ny teknik möjliggör nya sätt att använda samt leverera IT, trampar man oftast in på outforskade områden. Detta ger naturligtvis en ökad riskfaktor. Molnet och molntjänster har ansetts hålla en relativt hög säkerhet om man syftar på de större molnleverantörerna, emellertid har det visat sig i en nyligen genomförd undersökning att molnleverantörerna inte prioriterar säkerhet i första hand (Ponemon Institute, 2011). Vidare så anser mer än hälften av de undersökta molnleverantörerna att ansvaret ligger på kunden att säkerställa användningen av respektive molntjänst(ibid.).

Risker kommer alltid att finnas, genom de rätta förberedelserna kan man minska risken emellertid kommer alltid den mänskliga faktorn vara den svagaste länken när det gäller att säkerställa en god säkerhet (Rittinghouse & Ransome, 2010).

3.2.1 Risker inom datasäkerhetsaspekter

Sekretess och integritet

En väsentlig del vid användning av molnet är att säkerställa att obehöriga inte får åtkomst samt modifikation av befintlig information sker av misstag eller möjligtvis avsiktligt(Zizzis & Lekkas, 2010). För att se till att värdefull företagsinformation inte missbrukas menar Zizzis & Lekkas (2010) att man borde hantera detta genom att endast ge användare tillträde samt rättigheter till de respektive resurser som ska användas. Finns även en problematik gällande publika moln, eftersom infrastrukturen delas med andra användare finns risken att obehöriga får åtkomst till företagsinformationen eftersom varje kundinstans endast är separerad virtuellt(ibid.). Till följd av att kundinstanserna endast är separerade virtuellt finns det risk att genom ett säkerhetshål i en molnapplikation få obehörig åtkomst(ibid.). Zizzis & Lekkas (2010) betonar emellertid att det är molnleverantörens ansvar att skapa säkra virtuella instanser till kunderna.

Tillgänglighet

Eftersom molntjänster endast kan nås via Internet är den absoluta grundförutsättningen att man har en Internet-anslutning. Den största tillgänglighetsrisken överhuvudtaget kan man säga är bristen på en stabil Internet-anslutning. Risken minskar emellertid inte även om man har tillgång till en stabil anslutning. I en rapport från NIST (2011) med guidelinjer kring säkerhet och integritet kan tillgängligheten påverkas på flera olika sätt, rapporten nämner vidare att påverkan kan antingen vara temporär eller permanent. Exempelvis på risker som kan påverka tillgängligheten är avbrott i molnleverantörens utrustning, DoS-attacker (Denial of Service, t.ex. överbelastningsangrepp), naturkatastrofer samt att det finns även risk för att man helt eller delvist förlora företagsinformationen(ibid.). NIST (2011) menar emellertid att den största oron kring tillgänglighetsrisker är oplanerade driftstopp, i och med att risken för påverkan på företagsaffärer ökar.

För att helt skydda sig från ovanstående risker är svårt men det går att förbereda sig ifall det skulle bli aktuellt. NIST(2011) betonar viktigheten att själv kunna ha

möjligheten till att återuppta verksamheten inom ett kortare tidsspann ifall det skulle ske ett längre avbrott eller en katastrof.

Eftersom risken finns för en eventuell förlust av företagsinformation blev tre stora molnleverantörer i en artikel tillfrågade på hur de säkerställer tillgängligheten på kundernas företagsinformation ifall en olycka skulle ske (Söderlind, 2011). De tillfrågade molnleverantörer var Google, Microsoft samt Sungard.

Samtliga molnleverantörers infrastruktur är byggda för redundans, för att förhindra informationsförluster. För Googles och Microsofts del så sparas informationen alltid på separata platser medans Sungard ger varje kund en backup-konfiguration som är dedikerad endast till en kund(ibid.). Samtliga molnleverantörer betonar att de har hög transparens ifall ett avbrott skulle ske, de uttrycker vidare att som användare inte skulle märka av ett avbrott(ibid.).

Krypteringsolyckor

Kryptering används för att begränsa obehöriga att kunna läsa informationen man lägger ut i molnet. Algoritm skyddas informationen genom att göra den oläslig, man behöver i sin tur en nyckel som dekrypterar informationen till läslig igen (Heiser & Nicolett, 2008). I en rapport från Gartner rekommenderar de att man krypterar informationen man lägger ut, inte bara i transit utan även där den är lagrad (Casper, 2011). Även om kryptering är ett bra sätt att skydda det man väljer att lägga ut i molnet finns det en risk att man förlorar informationen. När en så kallad krypteringsolycka sker förstörs informationen och den går förlorad (Heiser & Nicolett, 2008). Risken för krypteringsolyckor ökar när man försöker skapa komplexa samt långa algoritmer, visserligen ökar skyddet om det fungerar felfritt emellertid menar Casper (2011) att det viktigaste är att informationen blir krypterad, inte hur den är krypterad. Sangroya et al. (2010) menar att risken att informationen förstörs i vissa fall ger upphov till att kunden inte vill låta informationen bli krypterad. Kryptering förespråkas emellertid fortfarande som det effektivaste alternativet för att förhindra obehörig åtkomst(Heiser & Nicolett, 2008).

3.2.2 Risker inom legala aspekter

Äganderätt till data

Oron över vad som händer med äganderätten till data man lägger ut i molnet har Gartner konstaterat i en rapport att den förblir oförändrad(Logan, 2009). Även om man lägger ut information ut i molnet så har man fortfarande skyldigheten att se till att informationen hanteras korrekt(ibid.).

Emellertid så menar Plummer (2010) att det fortfarande kan finnas oklarheter i molnleverantörers avtal över vad som utgör ens information. Vidare så anmärker Plummer (2010) på att det finns en brist med oberoende granskning i frågan. Utan granskning om avtalsvillkoren kan inte kunden bekräfta om de följs eller inte. Som i sin tur slutar med att kunden ofta tar molnleverantörens ord som fakta vid upphandling(ibid.).

Avtal

När det gäller att avtala om molntjänster måste man vara försiktig, risken är stor att molnavtalen är för enkla hävdar CIO Fokus (2011). Molnavtal kan ses som väldigt enkla och det beror på att avtalen endast är utformat efter specifika tjänster som inte går att anpassa samt som kan sakna garantier från leverantören kring områden som bland annat säkerhet(ibid.). Avtalen är viktiga eftersom där regleras detaljer bland annat som servicenivåer, påföljder vid brott mot delar i avtalet, prissättning, processer samt säkerhetskrav vilket medför att molnavtalens enkelhet skapar problem med att få de garantier som behövs(ibid.). CIO Fokus (2011) menar att det visserligen finns många molnleverantörer som är ovilliga att göra förändringar i molnavtal. Något som anses, kan vara det största misstaget man kan göra som blivande molnkund är att acceptera molnleverantörens avtal som de är samt tro att det kommer ge ett fullgott skydd(ibid.). CIO Fokus (2011) fortsätter emellertid betona att, ifall man inte hittar en molnleverantör som är villig att gå med på eventuella krav från kunden, kan det till viss del betyda att företaget ännu inte har mognat och är redo att ta steget ut för att börja använda molntjänster.

Lagar och regler

När det kommer till lagar och regelverk kan det ibland vara diffust och man finner svårigheter med att veta vad som gäller vid hantering av information i molnet. Överlag så är det komplext att flytta samt hantera information, i synnerhet personuppgifter emellertid är hanteringen av informationen relativ klar över vad som gäller, såvida informationen stannar inom Sveriges gränser. De största molnleverantörerna är däremot globala aktörer alltså finns det en stor risk att informationen flyttas utanför Sveriges gränser likaså utanför EUs gränser. Även om det är möjligt att begränsa genom avtal att exempelvis information endast får stanna inom EU uppstår det ändå en högre grad av komplexitet.

Enligt EU Direktivet 95/46 för skydd av personuppgifter fastslår man att det är förbjudet att flytta personuppgifter till ett land där man inte kan garantera motsvarande skydd vid hantering. Citerat från EU Direktivet 95/46,artikel 25:

> *"The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."*

Svantesson och Clarke(2010) menar att denna typ av bestämmelser begränsar väsentligt möjligheterna över hur molntjänster kan användas över gränser. Enligt Svantesson och Clarke(ibid.) så utgör bestämmelser likt EU Direktivet ett stort hinder för global utbredning och användning av molntjänster. Emellertid håller författarna med att artikel 25 av EU Direktivet 95/46 spelar en väldigt stor samt viktig roll för skydd av personuppgifter(ibid.).

Detta innebär att det blir enligt EU Direktivet förbjudet att flytta personlig information mellan EU och USA då det senare nämnda inte har samma krav gällande integritetsskydd (U.S. Department of Commerce, 2000). I och med att de större molnleverantörerna är amerikanskägda företag som håller driften till större delen i USA skapas ett stort hinder. För att överbrygga de skillnader som finns utarbetade det amerikanska handelsministeriet i samråd med EU kommissionen ett ramverk som benämndes ”Safe Harbor” (ibid.). Safe Harbor ramverket innehåller riktlinjer för hur man säkerställa att ett företag tillhandhåller korrekt skydd enligt EU Direktivet. Safe Harbor programmet godkändes av EU år 2000 och detta gav amerikanska företag möjligheten att enklare följa EU Direktivet(ibid.).

Gartner nämner emellertid i en ny publicerad artikel att vissa företag inte tycker Safe Harbor ramverket är tillräckligt robust vad gäller tillämpning, möjlighet till granskning samt oklara och luddiga termer (Bona & Ridder, 2011). Rapporten understryker att fastän molnleverantörer har tillämpat Safe Harbor ramverket, finns det ett flertal molnleverantörer som vägrar garantera att informationen hålls lokalt eller att ens tala om var informationen är sparad (ibid.). Detta i sin tur skapar en stor osäkerhet vilket definitivt drabbar molnleverantörerna negativt. Ett fåtal av de större molnleverantörerna har emellertid börjat göra avtalsenliga eftergifter i den meningen(ibid.).

Ramverk likt Safe Harbor underlättar en hel del men inte det mest effektivaste sättet eftersom det bara skyfflar undan grundproblematiken. Nelson (2009) menar att det ligger på regeringen i respektive land att utmana nuvarande politik och lagstiftning som kan förhindra tillväxten av molnet. Genom att regeringen tar initiativet och uppmuntrar molnleverantörerna till att experimentera med nya tjänster skapas mervärde menar författaren(ibid.). Nelson (2009) uttrycker emellertid att den här typen av problematik som exempelvis berör Internet policy har lagstiftare kämpat med över 15år. Däremot med tanke på molnets omfattning måste lagstiftningen kunna gå över gränserna vilket enligt Nelson (2009) anses vara dubbelt så svårt men fem gånger så viktigare(ibid.). Svårigheten där förklaras att det aldrig är simpelt att fastställa vem som är ansvarig för vad (ibid.). En ändring av detta är på väg, i en artikel som nyligen publicerades säger Neelie Kroes som är EU kommissionen högsta ansvarig för EUs Digitala Agenda, att EU vill skapa bättre förutsättningar för molnkunder samt – leverantörer (Rådmark, 2011c). Neelie Kroes nämner vidare att målet för EU är att det ska bli en ”molnaktiv” region och stärker sitt argument genom att hävda att EU kan påskynda utvecklingen och nyttjandet av ännu bättre samt fler molntjänster (ibid.). Likt det Nelson (2009) förklarade i artikeln så betyder detta att EU har axlat på sig ansvaret för att utmana och driva fram en tydligare molnpolitik som främjar molnanvändningen. Neelie Kroes menar vidare att de oklarheter som finns i dag ser hon främst inom följande tre områden: juridik, tekniska och affärsmässiga aspekter samt marknadens behov(Rådmark, 2011c).

3.2.3 Risker inom organisatoriska aspekter

Inlåsning

Molntjänster som fortfarande är ett relativt outforskat område och med molnleverantörernas snabba takt att erbjuda tjänster har det gett upphov till en viss inlåsning. Conway (2011) menar att varje tjänst som erbjuds idag har en unik metod för interaktionen mellan moln och applikationer, data och klient. Detta leder till att det blir mycket svårare att använda flera leverantörer samt att smidigt integrera med andra molntjänster likaså arv-system (ibid.). Inlåsning kan ses som attraktivt från ett molnleverantörperspektiv emellertid innebär en inlåsning för kundens del en ökad risk (Armbrust et al., 2009). Vidare så skriver Armbrust et al. (2009) att risken kan minskas vid konsolidering samt standardisering utav API;er. *(Application Programming Interface är en uppsättning med regler för hur programvara A kan kommunicera med programvara B)*

I en rapport från Gartner skriven 2010, nämner man emellertid att den ökade risken för inlåsning kommer troligt finnas kvar i ytterligare tre år innan det sker förbättringar (Plummer, 2010).

Ansvar och tillit

Problematiken kring integritetsskydd i molnet har visat sig vara en viktig fråga man behöver hantera. Enligt Pearson & Charlesworth (2009) kan man lösa det genom ansvarsförbindelse där varje inblandad part har ett ansvar gentemot respektive. Författarna föreslår att molnleverantörerna ska kontraktera ansvarsskyldigheten mellan kund och leverantör samt eventuell tredjepartsleverantör istället för termer och villkor för den utgivna molntjänsten(ibid.). Detta innebär att varje part får ett ansvar som blir lagligt bindande i varje led. Pearson & Charlesworth (2009) menar att ansvarsskyldighet genom kontraktering främjar förtroendet hos användaren. Pearson & Charlesworth (2009) argumenterar vidare att bristen på kontroll över vem och hur personlig information hanteras skapar misstänksamhet som i slutändan leder till misstro. Ansvarsskyldigheten genom kontrakt spelar i den meningen därför stor roll vid upprätthållning av lagar och regler rörande molnet samt molntjänster.

Coetzee & Eloff (2005) menar emellertid att tillit inte skapas genom lagligt bindande kontrakt. Författarna betonar att parter som har ett kontrakt med varandra, har indirekt tillit till respektive. Detta eftersom det rättsliga systemet finns emellan dem(ibid.). Coetzee & Eloff (2005) menar att tillit endast skapas genom att påvisa kompetens, ärlighet, säkerhet eller tillförlitlighet.

4. Resultat

4.1 Respondenternas syn på molnet och molntjänster

4.1.1 Definition av molnet och molntjänster

”Ja, det är en svår fråga, jag menar det, det är ju egentligen så pass omoget område så att det blir ju ganska bred definition. Jag skulle vilja säga att de är alla typer av tjänster som man kan leverera utan och ha egen investering i hårdvara och egentligen i mjukvara också, utan att man köper, grunden är ju egentligen inte bara tekniken för det kan göras på många olika sätt, utan det är hur man köper och hur man använder IT är det som jag tycker är det som karaktäriserar molntjänster. Man behöver i princip ingen egen infrastruktur eller kompetens på den infrastrukturen. Då är man nära en molntjänst.” ***– Respondent A.***

Respondent B menar att molnet och molntjänster kan vara många olika saker men huvudsakligen är det när man drar nytta utav en redan befintlig infrastruktur. Vilket respondenten fortsätter med att:

”[…] infrastruktur kan dels vara sladdar och det kan vara hårdvara med det kan ju också vara infrastruktur på en högre nivå som mjukvara.” ***– Respondent B.***

Respondent C definierar molnet som en bra möjlighet att lägga ut lösningar på ett ställe där man kan hitta en bra dynamik runt det. I likhet med samtliga respondenter hade även respondent E svårigheter att precist kunna definiera molnet och molntjänster men betonar att:

”I den mest grundläggande för mig så innebär ju molnet att det alltid att tjänsterna involverar nån typ av nätverkstrafik, det är liksom en grundförutsättning. Molnet som symbol liksom som har fått stå som namn över det, det visar ju nån typ av distribuerat nätverk i alla fall i mina ögon och normalt sätt Internet då. Och det molnet då får symbolisera ett avstånd mellan den som nyttjar en applikation och den som tillhandhåller en applikation eller en tjänst eller vad det nu kan vara. Så för mig är det ett grundkrav för att det ska få ett moln, molnet i sig eller att det ska vara en molntillämpning är att det finns ett nätverk, så att det finns ett visst avstånd då mellan konsument och tillhandahållare egentligen.” ***– Respondent E.***

Vidare så påpekar respondent E att man kan argumentera om en vanlig webbsida är en molntjänst eller inte samt ger exempel på Microsofts epost-tjänst Hotmail som oftast brukas tas upp som en tidig molntjänst. När det gäller just specifikt för molnet så menar respondent E även att:

”[…]eftersom det också är ett marknadsföringsord så blir det ju snabbt laddat med massa olika betydelser och alla leverantörer vill ladda det med sina definitioner. […] vad jag tycker är en vettig molntjänst, nånting som jag skulle snacka ”Cloud Computing” […] så skulle det innefatta en tjänst som är webb-baserad, en tjänst som stödjer flera, alltså som har som grundtanke egentligen att alla nyttjare av tjänsten använder samma kod-

bas […] om vi har en tjänst som alla får nyttja samma, dom kan ha olika abonnemang och så vidare kanske och utnyttjar olika delar av den, men vi har inte gjort anpassningar som är unika för en viss kund till exempel i kod-basen. Det är också ett kriterium tycker jag." ***– Respondent E.***

Ett annat nödvändigt kriterium för en välgjord molntjänst, nämner respondent E även att det ska finnas elasticitet, att det rent tekniskt sett finns en möjlighet att på ett enkelt sätt, vid behov kunna skala upp och skala ner förbrukningen eller kapaciteten i system. Vidare så menar Respondent E att det även beror på från vilket håll man tittar från.

"Sen beror det på lite om man ser det utifrån ett konsumtionsperspektiv eller ett leverantörsperspektiv också kan jag tycka att, som konsument så kan jag det vara, där så betyder moln att jag kan betala för min användning kanske. Jag betalar inte per CPU eller nått annat tekniskt som inte egentligen betyder nått för mig utan nånting som är verksamhets kopplat per användare eller per timme[…] nånting som ändå har en bäring på min verksamhet istället för o betala för hur många CPU är det? Eller hur mycket ram är det? Så att det blir en mer verksamhetsnära koppling till vad som kostar. Medans om man är från leverantörssidan så är det snarare då kopplat kanske till hur arkitekturen är och så vidare, att den är liksom molnanpassad på ett vettigt sätt annars är det "fake-moln" på nått sätt (skrattar). ***– Respondent E.***

Där respondent E ännu en gång betonar att molnet och molntjänster är svårdefinierat eftersom det helt beror på i vilket perspektiv man tittar från.

4.1.2 Säkerhet och risker i molnet och molntjänster

När det gäller säkerhet kring molnet så svarar respondent A så här:

"Generellt sätt så anser jag så här, det är väl troligt att en professionell aktör med molntjänster, dom lär ju sig hur dom ska skydda data och sin tjänst på ett bättre sätt än jag kan göra själv, om inte IT och leverans av molntjänster är min huvudsakliga verksamhet, så kan man säga. Det finns ingenting att köpa via molnet som gör den mindre säker än att jag gör mina egna lösningar. […] Däremot så olika aktörer på molnmarknaden varierar ju väldigt mycket, hur mycket förtroende jag har för dom." ***– Respondent A.***

Vidare så menar respondent A att de företag som gör mer infrastrukturnära molntjänster har kommit längre än övriga aktörer eftersom det är ett mycket äldre sätt och leverera molntjänster på. Respondent A betonar dock att:

"Det är mycket mer upp till mig som användare om det blir säkert eller inte. […] men tittar man på modernare tjänster där jag egentligen lägger min affärsinformation hos molnleverantören. Då är det ju andra saker som kommer i spel egentligen, om jag litar på dom eller inte, det är ju vad dom har för policys och rutiner kring data, ägarskap och sånna här saker." ***– Respondent A.***

Vidare så fortsätter respondent A med att betona att god säkerhet inte bara handlar om det tekniska eftersom alla stora molnleverantörer idag(med något undantag) håller en bra nivå när det gäller säkerhet inom de tekniska aspekterna.

Respondent B menar på att molnet kan vara säkert givet att leverantörerna kan på bästa möjliga sätt garantera att det är säkert.

När respondent C blev tillfrågad om molntjänster kunde anses säkert, handlade det mer om mognad och gav en liknelsen med att betala över Internet:

”De är lite samma, anser man att det säkert att betala med kreditkort över nätet? I början så var det ju, fanns det problem med det, samtidigt som nu när det har mognat så känner jag mig väldigt trygg med att betala via nätet.” ***– Respondent C.***

Men betonade vidare att:

”Däremot så vet jag inte om jag skulle kunna rekommendera för någon av våra kunder att lägga ut företagskänslig information i molnet. Jag tror där är jag för osäker och kan för lite om det för att göra dom rekommendationerna. Men att lägga ut nån typ av applikation som hanterar […] annan information som kanske inte har med den känsligaste affärsinformationen och göra så att jag känner mig rätt trygg ja.” ***– Respondent C.***

Respondent D menar att det gäller att vara uppmärksam när det handlar om säkerhet och visade förtroende för de stora molnleverantörerna att de uppfyller de krav som behövs.

Respondent E menar vidare att molnet och molntjänster inte nödvändigtvis behöver vara osäkrare än egna system inom företagets väggar och fortsätter med att det är möjligt att få det lika säkert eller säkrare med att lägga data i molnet än att ha det i sin egen dator. Däremot betonar respondent E att det finns ett antal känsliga punkter där säkerheten kan brista.

”Ett av dom är ju såklart att skicka trafik över ett nätverk. Gör man det vettigt så krypterar man och så vidare men så klart det är ju ändå en säkerhetsrisk att liksom andra kan komma åt det och sådär. Så där krävs ju att man självklart använder kryptering av all typ av datatransfer […] En annan typ av säkerhet handlar ju om upptid och tillgänglighet och så vidare. […] Det räcker att nån gräver upp en kabel utanför eller det räcker att en DNS-server i USA inte funkar eller nått sånt där om vi har våra grejer där så att vi kanske inte kommer åt våran data längre.” ***– Respondent E.***

Respondent E menar att det visserligen är en ökad risk men betonar att:

”Samtidigt så måste man vara väldigt medveten om vad man köper. Det räcker inte bara och skaffa sig ett konto på Microsoft Azure eller på Google eller hos Amazon och sen nu är jag i molnet, nu är allting lugnt.” ***– Respondent E.***

Respondent E menar vidare på att molnet kan vara säkert för de allra flesta tillämpningarna.

”För det finns liksom ingen uppenbar sak generellt i moln som gör att det inte skulle vara säkert där, däremot så är det liksom inte en… Det finns ju inga genvägar egentligen till och fixa ett säkert system. Det är svårt oavsett hur man gör och det är svårt om man gör det i molnet och det är svårt om man gör det utan molnet också” ***– Respondent E.***

När frågan kom som fokuserade på risker istället menade respondent A att:

”Största risken är ju det här att, i många företag är ju information kanske den mest en utav den viktigaste resursen man har särskilt i kunskapsintensiva företag, så att risken är ju där att jag lägger min information hos nån annan och jag förlorar delvis kontrollen över den. […] En risk jag kan se är att jag vill avsluta mitt samarbete med molnleverantören, hur får jag tillbaks min information? Och hur får jag tillbaks den på ett format som är meningsfullt för mig? Säg att du har en jättestor kunddatabas, nu kanske enkel information, men vi tar det som exempel ändå med miljoner kunder och köp historik, och jag får jag tillbaks den i filformat i princip då från en tjänst. Ja, det är inte så lätt kanske och byta till nått annat.” ***– Respondent A.***

Respondent A menar att det kan innebära en viss inlåsningseffekt och anser det vara den största oron man egentligen kan ha. Vidare så nämner respondent A att det beror även mycket på vad för typ av avtal man har. Om det är en hyrd infrastruktur det handlar om kan man oftast hämta hem den egna infrastrukturen och betonar att det intressanta i den risken är:

”[…] när man pratar om software as a service på riktigt alltså. Det är där man kan ha den typen av avtal och då tycker jag definitivt det ligger på molnleverantörens ansvar och det är ett krav man ska ställa. Att man kan få ut sin data och säker på att den inte finns kvar nånstans hos molnleverantören också.” ***– Respondent A.***

Respondent B menar o andra sidan att:

”Ja, den största risken är ju att man inte har kalkylerat på risken, skulle jag säga. Vet man inte när man går in och köper tjänsten vad det är egentligen leverantören står för och vad dom egentligen lovar dig, om man inte vet det och det värsta händer för dig och du inte har då liksom behandlat risken innan. Det är då du är rökt, skulle jag säga. Det är egentligen den största risken att du inte vet vad du ger dig in på, skulle jag hävda.” ***– Respondent B.***

Respondent B menar även här att avtal är viktig del och fortsätter vidare med att ansvaret ligger lika mycket på båda parter.

”[…] jag har ju själv tagit ett aktivt beslut att utnyttja tjänsten så från början är ju ansvaret mitt, skulle jag tycka ändå. […] Ja, alltså dom avsäger sig allt ansvar, då är det

mitt ansvar att jag går med på det eller ej. Att jag köper, att jag accepterar den dealen ändå." ***– Respondent B.***

Respondent C anser att risken är just osäkerheten på vem som hanterar och kommer åt informationen man lägger upp i molnet.

"Vem det är som garanterar exempelvis om det finns information med sekretess, i att den sekretessen och dom bitarna upprätthålls i molnmiljö. Hur avtalen kan regleras för att säkerställa detta då. Jag ser väl också risken att även om du har ett avtal som gäller rent juridiskt, hur följer du upp det beroende på lättillgängligheten via att du lägger ut nånting i en molnmiljö då? Vem som säkerställer […] åtkomst möjligheterna till den här molnmiljön då." ***– Respondent C.***

Respondent C menar vidare på att den upplevda osäkerheten har mycket med just hanteringen av informationen och vem som tar ansvar för den.

"Det finns ju seriösa och mindre seriösa aktörer. Och tidigt i en ny teknik eller en ny plattform så kan antalet mer oseriösa leverantörer, nu kanske jag inte pratar om sånna som medvetet begår brott, utan sånna som inte har samma muskler att tänka på vissa aspekter när det gäller säkerhet och dom bitarna som agerar som kanske inte är lika seriösa på det sättet och det skulle kunna öka riskerna till att informationen hamnar fel då." ***– Respondent C.***

Respondent D menar att den största risken inte nödvändigtvis är att någon obehörig kommer åt informationen eller att informationen försvinner utan den största risken, sett ifrån ett slutanvändarperspektiv, är att själva användningen av en molntjänst blir krånglig.

"Att det liksom inte blir effektivt och jobba med det. Finns ju massa tekniska hinder liksom, […] man ska ju inte märka att det ligger någon annanstans och det tror jag är det största hindret. […] att du får logga in massa gånger och det är krångligt, alltså det är inte lika lätt som när du har den i ditt eget nätverk, för då är behörigheter uppsatta och allt sånt är redan klart. Det blir helt enkelt ett snäpp krångligare då. Och det försöker man ju få bort och man har kommit en viss bit på väg men jag tror ju att det ändå inte bara är sådär (knäpper med fingrarna), så lätt och göra det." ***– Respondent D.***

Respondent E menar att det finns ett par risker som är riktigt stora.

"Den ena är just det här att det finns liksom ett avstånd, att man är nät-bunden då. Så att nätverksaccess går ju ner det är ju inte jätte ovanligt. Det är ju liksom den största tillgänglighetsrisken skulle jag säga, men den andra stora risken som jag ser det är ju att man, det är inte så mycket att man delar kanske infrastruktur och sånt där utan att […] man lägger en stor del av sin verksamhet och sina stödsystem hos en leverantör som man kanske inte har så jätte bra kolla på." ***– Respondent E.***

Respondent E menar vidare att om man vill ha en bra infrastruktur måste man då vända sig till dom stora molnleverantörerna men betonar emellertid att man blir:

" […] en liten fisk i en väldigt stor sjö […] och man kan inte sitta och snacka med deras teknikchef om hur dom har byggt upp allt så där, man får inte den här personliga relationen och därför kan man inte skaffa sig en jättebra koll på vilka säkerhetsrisker eller liksom "pre-cautions" dom har tagit utan man får försöka lita på vad det står i deras dokument och deras webb och det är ju en stor risk." ***– Respondent E.***

Respondent E menar vidare att man inte riktigt får den nära relationen som man skulle ha fått om man arbetat med en lokal partner. Respondent E nämner vidare problematiken att:

"Man vill gå till en stor leverantör för o få bra grejer men är man med sån stor leverantör då är man själv liten i jämförelsen med dom. Det är väl den största risken tycker jag. […] det finns ju liksom ett skevt maktförhållande där på något sätt som kan vara lurigt. Sen finns det ju andra risker också, men jag tycker att dom här är de största." ***– Respondent E.***

4.2 Kundernas uppfattning om molnet och molntjänster

Efter att respondenterna fått frågor kring deras egen syn på molnet och molntjänster kom tillfället att fråga hur respondenterna har tolkat deras kunders uppfattning, samt vad kunderna känner för molnet och molntjänster.

4.2.1 Främsta anledning med att börja använda molntjänster

Främsta anledningarna för att börja använda molntjänster identifierades som att slippa investera i hårdvara och kompetens, kostnadsbesparingar samt flexibilitet. Samtliga respondenter förklarade att det är väldigt kostsamt att driva en egen IT-infrastruktur. Respondent B nämner att de kunder som har IT som sitt primära affärsområde väljer molntjänster eftersom:

"Dels för att det kan finnas paketerade tjänster som redan finns, så dom slipper att investera i utvecklingstid för att göra motsvarande själva." ***– Respondent B.***

Respondent E nämner emellertid att de kunder som inte är ett IT företag oftast inte vill investera i något som inte är relevant för kärnaffärsområdet. Respondenten uttrycker att:

"Man vill inte sätta sig i det, det känns inte som kärnbusinessen, man vill inte investera pengar i det helt enkelt" ***– Respondent E.***

Anledning att vilja börja använda molnet och molntjänster har även identifierats som att kunderna vill ha ökade flexibilitet i verksamheten. Bland annat i deras systemanvändning, respondent C nämner att det som attraherar kunderna är:

"att kunna variera datakraften över tiden, kunna se till att bara ha den kapaciteten man behöver för ett visst tillfälle" ***– Respondent C.***

Flexibiliteten att kunna variera datorkraften ses även som en kostnadsbesparing eftersom man:

”då betalar rätt summor, dvs. att undvika att betala för över-kapacitet och samtidigt undvika i att hamna i problem vid eventuell underkapacitet” ***– Respondent C.***

Kunder som är IT företag och själva bedriver någon typ av utveckling, har attraktionen för molnets flexibilitet även varit följande:

”dessutom ser vi företag […] som vill kunna prova saker, då är ju ett snabbt sätt att kunna få upp test-miljöer” ***– Respondent A.***

Respondent E menar vidare att en ytterligare anledning med att börja använda molntjänster kan vara ifall man har en partner och/eller kund som redan idag använder molnet. Det företag då vill underlätta är själva integrationen med sina parter.

4.2.2 Uppfattning om molnet och molntjänster

Uppfattningen Acandos kunder har om molnet och molntjänster som identifierats är väldigt varierande och respondent B menar att det inte finns någon entydig uppfattning.

”många har olika definition på vad molnet är för det första. Och saken är ju, det är ju ingen som har fel definition. Men det är ofta ur deras uppfattning om vad det är, som gör också vad dom har för uppfattning om hur dom ska använda det, det återspeglas så att säga.” ***– Respondent B.***

Respondent E menar vidare att Acando har ett väldigt brett spektrum kunder där det huvudsakligen finns tre typer av kunder. *1.* De kunder som är väldigt entusiastiska och vill börja använda molnet för att testa det. *2.* Vidare finns det kunder som är mer av den traditionella typen där man går försiktigt fram. Man vill helst inte vara först ut och ser gärna hur andra företag har handskats med molntjänster innan. *3.* Sista typen av kunder är den direkta motsatsen till både typ 1 och 2, som absolut inte kan tänka sig att använda molntjänster eftersom man inte kan förlita sig på någon annan att hantera företagets information.

Respondent D menar vidare att emellanåt kan finnas kunder med nästan känslomässiga skäl inte kan förmå sig att lägga ut information ute i molnet.

Respondent A betonar emellertid att:

”Det varierar mycket. Jag upplever att dom svenska kunderna vi har, dom är faktiskt lite senare […] Sverige brukar vara i framkanten men här ligger vi nog kanske lite efter USA. […] Däremot går det ganska trögt för dom stora bolagen tycker jag, här i Sverige. Det är nog generellt egentligen att stora, traditionella bolag är senare på detta.” ***– Respondent A.***

4.2.3 Upplevda oron och hur den hanteras

Den mest återkommande oron har bland annat visat sig vara kring säkerheten, mer specifikt handlar det om datasäkerheten. Följande frågor har identifierats från kunderna som orosmoment inom datasäkerhet:

- Behåller man rättigheterna till ens data?
- Hur kan man vara säker på att ingen obehörig kommer åt data?
- Hur kan man vara säker på att det är bara behöriga som kan läsa det?
- Hur kan man vara säker på att behöriga verkligen kan läsa det?
- Hur kan man vara säker på att molnleverantören inte gör något fel?

Respondent E menar vidare att kunder som övervägt kryptering för att säkra sin data, skapas det ett ytterligare orosmoment. Respondent E förklarar vidare att man blir orolig över ifall något skulle hända med krypteringen, vilket i sin tur leder att möjligheten att komma åt sin data försvinner. Krypteringsproblematiken kan i enstaka fall alltså upplevas som värre än att andra kommer åt företagets data, fortsätter respondent E med.

Den oro som kunderna upplever behöver hanteras och respondent B menar att man borde behandla oron med full respekt. Respondent A menar vidare att man borde bemöta oron direkt genom grundliga diskussioner kring oron som finns för att kunna hantera den på bästa sätt.

Respondent B nämner emellertid att:

> **"***känner kunden en viss oro för det, så har ofta kunden själv en alternativ tillvägagångssätt så att säga. Hur man skulle kunna lösa samma sak. […] men tycker kunden, ja men det här låter intressant, kan inte ni titta närmare på det och förklara för mig då och förtydliga vad det erbjudandet verkligen är? Ja men självklart då gör vi ju det.* ***– Respondent B.***

Respondent E menar vidare att det enda man egentligen kan göra är att prata och förklara för att öka medvetenheten.

> *"Ja absolut, man får prata mycket om det och förklara. Berätta vad andra har gjort och berätta lite sånt här; Det här är bra exempel på molnanvändning kanske. Men det här är också riskerna då. Känns dom acceptabla? Känns dom inte acceptabla? Om dom känns att dom skulle kunna vara acceptabla, kanske vi ska göra något testskott eller göra en förstudie."* ***– Respondent E.***

Respondent B menar vidare att medvetenheten om vad man köper är väldigt viktig. Respondent E betonar vikten med att kunna ta initierade beslut. I den här typen av frågor är det bättre att ta faktabaserade beslut än känslomässiga, fortsätter respondent E med.

Respondent E har emellertid fått uppfattningen att en del kunder tror att information ligger säkrare inom företagets väggar. Respondent E ger ett förslag att man borde börja

med att titta till den egna verksamheten och dess säkerhet samt ställa det i jämförelse med molnet. Respondent E förklarar tydligare att:

”Det finns utspridd tanke om att man alltid är säker om man har det själv. Men ofta är det ju, eller det är inte alltid ofta det är så, […] ,där kanske databasadministratören kan läsa all data i alla databaser. Eller alla systemtekniker. Alla utvecklare kommer åt all data i alla databaser för att dom har tillgång till root-lösenordet till exempel. Man reflekterar ju inte ens över den grejen medans man är jätteoroad att nån annan på andra sidan världen kan läsa nånting som kanske redan är krypterat. Man måste liksom ställa dom här sakerna i paritet till varandra så man inte bara jämför en teoretisk idealbild av världen mot moln och sen så vad det gäller den egna så jämför man det inte med nånting utan man kanske har en ganska, alltså så man på nått sätt försöker öppnar ögonen, vad har vi idag? Vad är det här molnet? Hur förhåller dom sig till varandra? Skillnader? Likheter och sånt där. Då kanske man ser att det inte är så jättestor skillnad.” ***– Respondent E.***

Respondent A har emellertid uppmärksammat från diskussioner med kunder att tryggheten har ökat för molnet, nu när kunderna själva får se vad andra företag gör. Respondent A uttrycker att:

”Det blir nog litegrann av en ”ketchupeffekt”, när man hör att fler och fler gör det, så vill man göra det själv också.” ***– Respondent A.***

Genom diskussioner med kunder har respondent A även lagt märke till att den oro som finns kan till stor del bero på en personlig oro. Respondent A förklarar så här:

”*Jag tror många beslutsfattare är oroliga över att personligen göra bort sig om dom bestämmer att välja molntjänsten, att det är dåligt för deras karriär, förstår du vad jag menar? Om man väljer det traditionella som man gjort innan då har man inte gjort fel. Men säger man att nu går vi över till den här tjänsten och sen visar den sig inte hålla. Då är man rädd att det ska drabba en negativt*.” ***– Respondent A.***

Respondent A har tolkat ovanstående som att det ofta handlar om en större upplevd risk, än en faktisk risk.

4.3 Utmaningar

När respondenterna frågades om vad de ansåg vara den största utmaningen i molnprojekt svarade majoriteten att avtal är den största delen som kan ge en extra utmaning. Likaså var säkerhet en utmaning men respondenterna betonade emellertid att säkerhet är ett svårt område oavsett om det handlar om att säkerställa en molntjänst eller ej.

Samtliga respondenter ansåg avtal för molntjänster vara en stor utmaning. Respondent A uttrycker att det svåra bland annat är:

”vilken typ av avtal man ska ha och vem som garanterar vad är ju intressant. För ofta vill ju kunden ha ett avtal med oss där vi garanterar allt men vi behöver i sin tur en

leverantör och vi måste vara transparenta däremellan för att vi kan ju inte påverka vad t.ex. Microsoft gör som är en stor partner. Så att där kan ju vara en utmaning." ***– Respondent A.***

Respondent B fortsätter vidare med att nämna att utmaningen med avtal ligger även i att kunna förklara dessa till kunden:

"Utmaningen ligger i och förklara varför vissa saker är som det är, skulle jag hävda." ***– Respondent B.***

En annan utmaning handlade om säkerhet. Samtliga respondenter var överens att utmaningen med att skapa en god säkerhet inte på något sätt är mer komplext i molnet, respondent B svarade bland annat så här:

"Det är svårt oavsett om molnleverantörer är inblandade eller ej. Det är ju ändå nånting man måste ta med i beräkningen då beroende på vad det är för system då. Jag ska nog inte hävda att det är svårare med molnleverantören än vad det är på vanligt sätt, det är svårt ändå så att säga." ***– Respondent B.***

Respondent A nämner ytterligare att integrationen med molntjänster kan bidra med en del utmaningar:

"Sen tekniskt så är det ju det här ofta med integrationen. De är ju fortfarande ganska omoget(molnet). Hur man integrerar med säkerhetstjänster, kundens befintliga infrastruktur och system och sånt där. Det är ju fortfarande mycket av en utmaning." ***– Respondent A.***

När det gäller att integrera molntjänster med kundens befintliga infrastruktur betonar respondent E att det alltid kräver eftertanke samt att man gör det ordentligt men anser ändå inte att integrationen blir svårare i en molnmiljö.

Respondent E nämner vidare att utmaningarna inom till exempel avtal ligger till större delen i molnleverantörernas "SLA" (service level agreement). SLA är avtal mellan kund och leverantör där man reglerar vad leverantörer står för och vad som händer när det inte är som det borde vara, till exempel drift, upptid och tillgänglighet. Problematiken i ovanstående menar respondent E att det återigen kan leda till, som tidigare nämnt, "stor och liten – problematiken". En större molnleverantör har till större delen inget förhandlingsutrymme. Respondent E förklarar att:

"Så där har man ingen, upplever jag i alla fall, ingen eller väldigt lite möjlighet till att få saker i ett avtal som reglerare. Dom är ofta pigga på att kanske visa; Ja men du kan uppnå en högre tillgänglighetsfaktor genom att göra så här, så här och så här men vi kan inte avtala om det. Det är ju ett bekymmer för en del. " ***– Respondent E.***

Respondent B menar vidare att när det gäller molnleverantörernas SLA gäller det att vara uppmärksam och så behjälplig som möjligt för att kunden ska känna sig trygg.

4.3.1 Sammanfattning av samtliga molnprojekt

Respondenterna ombads även att försöka sammanfatta samtliga molnprojekt de har deltagit hittills. Frågan ansågs väldigt svår att kunna svara på eftersom samtliga projekt varierar väldigt mycket. I frågans svåra natur svarade emellertid respondent A att om det gäller argument till att börja använda molntjänster så letar oftast större traditionella företag efter kostnadsbesparare för att kunna stötta arbetsstyrkan vilken är rörlig och global. Respondent A nämner vidare att molntjänster spelar en väldigt bra roll i ovannämnda situationer.

Respondent E sammanfattar med att molnet och molntjänster fortfarande känns som ett nytt område därav kan det fortfarande ge upphov till att man upplever ”svart/vitt - mentaliteten” som ofta visar sig hos ny teknik, några är alltid för och några är alltid emot. Respondent E menar vidare emellertid att molnprojekt egentligen är helt vanliga IT-projekt eller verksamhetsprojekt som man utför. Respondent E menar att det bara är en ny komponent man ska förhålla sig till:

> *”Jag tror att det är ytterligare en komponent liksom i IT landskapet som man ska förhålla sig till och ibland är den lämplig och ibland är den inte lämplig. […] Det är bara det att en ny komponent är med och man blir så tagen av den så man kanske glömmer bort och göra alla bra saker som man brukar göra. Finns en viss risk för det kanske.”* ***– Respondent E.***

4.4 Juridik

Legala-aspekter har visat sig vara en stor del utav utmaningarna man har stött på. Lagar och regler är inte helt uppenbara när det handlar om molntjänster. Det är mycket att ta i akt eftersom det ofta inte är 1 plats på 1 server molnleverantören sparar all data på. Data kan i många fall sparas utanför Sverige. Respondent A menar att avtalen för molntjänster inte är anpassade för lokala förhållanden (Givet att det är en icke-svensk aktör). Av den anledningen måste man ta hänsyn till att data även kan sparas utanför EU. Respondenterna menar vidare att ansvaret ligger på en själv och se till att man följer lagar och regelverk.

> *”[…] det får man ta hänsyn till men det blir ju som ett krav som alla andra. Jag ser väldigt den utmaningen för mig och andra på Acando som jobbar med det här att utbilda andra om vad som gäller.”* ***– Respondent A.***

Respondent C menar vidare på att utmaningen även ligger i att få ihop avtal som man kan känna sig trygg med.

Respondent C nämner den egna önskan att kunna skriva avtal som är hållbart reglerade gemensamt över världen, vilket minskar risken att tappa någon verkan för att det finns skillnader i olika länder. Respondent C betonar emellertid att mognadsfaktorn för att reglerera hållbara avtal världen över inte har kommit riktigt än då man först och främst behöver titta på skillnaderna samt testas i mindre skala.

När respondenterna blev frågade hur de ansåg molnleverantörernas avtal passade ihop med lagar och regelverk i de många länder molnleverantörerna opererar i, menar respondent E att de allra stora molnleverantörerna klarat av det bra och tillhandhåller oftast en bra dokumentation gällande lagar och regelverk.

”Så uttrycker sig dom flesta tycker jag att, dom garanterar inte att; Använd oss så funkar det. Så bryter du inte mot lagen eller sånt där. Men dom säger så här att; Vi ger dig möjligheten att följa lagen. Såvitt vi känner till så kommer du inte bryta dom här och dom här reglerna om du använder oss, om du använder oss på rätt sätt. Men det är upp till dig själv och se till att du använder oss på rätt sätt.” ***– Respondent E.***

När det gäller de mindre molnleverantörerna menar respondent E att de inte har så bra kontroll över vad som följer lagarna samt regelverken och vad som inte följer. Respondent E tror att det kan bero på att de minsta aktörerna saknar ett koncept av att dela till exempel användaruppgifter mellan USA och EU. Respondent E tillägger att det borde vara ett rudimentärt krav oberoende storlek.

Respondent E fortsätter med att betona:

”sist så är den som nyttjar tjänsten som beställer och det är den som är avtalspart som måste tillse att dom lagar som gäller för den aktören att dom verkligen uppfylls och dom gör väl vad dom kan där dom stora(molnleverantörer). […] Dom vill inte göra nånting där dom inte kan teoretiskt sätt göra att det blir lagligt tycker jag.” ***– Respondent E.***

Vidare menar respondent C även att lagstiftningarna släpar efter då ny teknik eller nya lösningar uppkommer. Anledningen till ovannämnda menar respondent C är att nya lösningar ofta kommer in på områden vilket tidigare inte varit möjliga att utreda, vilket initialt kan ge upphov till att vara en risk.

Respondent A förklarade tidigare att Sverige låg lite efter i sin användning av molntjänster emellertid betonar respondent A att det inte är de legala-aspekterna som har bromsat Sveriges användning av molntjänster.

4.5 Molnets och molntjänsters framtidssyn

Gällande framtidssynen var samtliga respondenter överens med att framtiden var ljus för molnet och molntjänster. Användningen kommer att öka rejält menar respondent A, samtidigt kommer molntjänsterna rationaliseras ytterligare för företagen fortsätter respondent B. Respondent E menar vidare att detta i sin tur kommer leda till ökad standardisering och konsolidering. Respondent A fortsätter att det som krävs är att först och främst gå mer mot standardisering av interoperabilitet samt säkerhet innan det verkliga genombrottet kommer.

Respondent D menar att man inte längre kommer att reflektera över vad som är acceptabelt att flytta till molnet allteftersom de tekniska- samt säkerhetsproblemen minskar eller försvinner helt.

Respondent E fortsätter vidare med att det troligt kommer en mindre eller större backlash. Respondenten menar vidare att det är det enda sättet för att kunna hitta den rätta nivån över hur mycket samt vad man kan lägga ut i molnet. En mindre eller större backlash kommer medföra att:

”man hittar bra strategier på vad som ska ligga i molnet, vad vi ska lägga hemma, vad vi behöver ha på dubbla ställen och så där då, det tror jag vi kommer göra” ***– Respondent E.***

Emellertid menar respondent C att innan molnet och molntjänster riktigt kan slå igenom ligger den främsta utmaningen i att verkligen ta ställning till och lära sig mer om vad för möjligheter molnet kan frambringa.

Avslutningsvis när det gäller vad molnet kommer ha för påverkan i framtiden uttrycker respondent A att:

”Jag tror investeringarna i de egna IT-avdelningarna som håller den typen av miljöer kommer minska ganska mycket. Det kommer och påverka IT-avdelningens roll mycket, det blir väldigt annorlunda. Vi som leverantörer kommer också behövas påverkas en hel del. Dock tror jag för Sverige att den här stora förändringen ligger nånstans 4-6 år bort kanske innan det verkligen har slagit igenom […] slagit igenom i vardagen så att säga.” ***– Respondent A.***

5. Diskussion

Valet att intervjua konsulter för empirin istället för företag(slutkunder) innebar att jag endast haft tillgång till andrahandsinformation. Jag skulle ändå hävda att det har varit ett bra val eftersom konsulterna på Acando har både haft expertis kring de mer molnspecifika frågorna samt erfarenheten från att tillsammans med sina kunder arbetat med komplexa frågor gällande molnet och molntjänster.

Här nedan kommer jag att diskutera resultatet och den skrivna litteraturen i de områden som identifierades i början av studien.

Definitionen

Samtliga respondenter hade svårigheter att definiera molnet och molntjänster eftersom det kunde betyda många olika saker beroende på vilket perspektiv man tittar från som respondent E bland annat uttryckte. Även om respondenterna hade svårighet med att precist kunna definiera en molntjänst, anser jag att man ändå hade en samlad vy över vilka grundförutsättningar det är som utgör en molntjänst. Dessa kunde sammanfattas följande; den tydligaste förutsättningen som kunde identifieras var att man drar nytta av en redan befintlig infrastruktur. Det innebär att man inte behöver investera i en infrastruktur. En annan samlad förutsättning var att det på något sätt involverade nätverkstrafik. Respondent A menade emellertid att det inte bara handlar om tekniken. Likt Gartners definition (Plummer et al. 2009. s.2) betonar respondent A att det är hur man köper och hur man använder IT som karaktäriserar molntjänster. Emellertid finns det en del tekniska aspekter som utgör en molntjänst vilket är minst lika viktiga. Respondent E nämner en annan grundförutsättning för en molntjänst var bland annat att det ska finnas elasticitet dvs. att det är rent tekniskt sett möjligt att på ett enkelt sätt kunna skala upp och skala ner resurser vid behov. I både Gartners och NISTs definition var elasticitet en viktig grundförutsättning(Smith & Cearley, 2010).

Säkerhet och risker

Säkerhet och risker har visat vara en väldigt stor del när man pratar om molnet. Samtliga respondenter nämnde att säkerheten nödvändigtvis inte behöver vara lägre bara för att man lägger ut information i molnet. Respondent A nämnde att risken ofta upplevs mer än vad den faktiska risken egentligen är, vilket även Gartner konstaterade(Casper, 2011).

Säkerheten har uppfattats som relativt hög hos molnleverantörerna enligt respondenterna. Till viss del bättre än den man har i det egna företaget. Men undersökningen som Ponemon Institute(2011) utförde, visade det sig vara att säkerheten kom i andra hand. De undersökta molnleverantörerna hävdade även att säkerheten låg på användarens ansvar, jag skulle emellertid hävda att det verkar finnas ett verkligt behov för företag att själva behöva se till att man säkerställer användningen, om molnleverantörerna inte kan garantera att säkerheten prioriteras.

Risker inom datasäkerhetsaspekter som identifierades kan jag tycka tillgängligheten vara den mest kritiska risken eftersom den är absolut svårast att förutspå. Även om

dataförluster kan ske är min uppfattning att, i alla fall de stora, leverantörerna håller hög nivå av redundans i sina infrastrukturer.

En intressant observation som gjordes var att det även i vissa fall framkom en personlig oro som bidrog till osäkerheten. Oron över att själv som beslutsfattare drabbas negativt ser jag som en onödig oro eftersom om man gör de förberedelserna som krävs för att säkerställa en molntjänst har man då, anser jag, ingen anledning till att vara oroad.

Vidare så uttryckte respondenterna att i rollen som konsult endast kan respektera kundens oro över de risker man kan utsättas för vid molnanvändning, det gäller att vara så behjälplig som möjlig. Konsulternas roll är att öka kunskapen så man som kund kan bli mer medveten ifall en risk är acceptabel eller inte. Respondent B uttryckte en väldigt viktig poäng gällande säkerhet och risker, vilket jag stödjer fullt ut, den största risken man kan utsätta sig för är att inte kalkylera på risken alls.

Utmaningar

Man kan med stor säkerhet säga att molnet har bidragit med en utmaning. De utmaningar respondenterna ansåg vara mest utmanande samt viktigast att ta itu med var avtalsmässiga utmaningar, säkerhetsmässiga utmaningar samt utmaningar med integration bland annat som integration med säkerhetstjänster och system. När det gäller avtalsmässiga utmaningar så svarade samtliga respondenter att service nivå-avtalen är svårast när det kommer till att få saker i ett avtal som reglerare när det kommer till de större molnleverantörerna. Respondent E uttryckte det som stor och liten – problematik. Det svåra med den här typen av problematik är att få klart för sig vem som garanterar vad. Enligt CIO Fokus(2011) berodde det på att molnavtal var utformade efter de specifika molntjänster vilket gör avtalen i sig enklare. Som respondent B uttrycker finns det en utmaning rörande avtal som bland annat konsulter har, att kunna förklara varför vissa saker är som de är till kunder. Vilket jag skulle anse att kunna bli betydligt bättre om man ökade medvetenheten hos företagen rörande denna typ av problematik.

Juridik

Inom detta område har jag fått uppfattningen att det är här som den mest oklarheten befinner sig. Frågor som rör bland annat äganderätt av data samt var företagsinformationen hamnar som har varit den största upplevda oron bland Acandos kunder. Gartner har dock konstaterat att vad gällande äganderätten så förblir den oförändrad(Logan, 2009). Enligt Plummer(2010) var det fortfarande oklarheter även här gällande molnleverantörernas avtal över vad som utgör ens information. Så återigen kommer problematiken med avtalen molnleverantörerna har.

Gällande gränsöverskridande överföringar av information, anser respondenterna att de stora molnleverantörerna har skött sig bra med att tillhandhålla dokumentation gällande lagar och regelverk. Regelverk likt EU Direktivet 95/46, har EU skyddat sina

medborgare när det gäller hantering av personlig information utanför EU, enligt artikel 25 av direktivet.

Även om tillämpningar likt Safe Harbor underlättar överföringen och säkerställer hanteringen för personliginformation utanför EUs gränser anser jag det emellertid inte vara ett hållbart alternativ. Om ändringar ska ske borde det ske från grunden. Nelson(2009) påpekade att ansvaret låg på varje regering i respektive land att utmana den nuvarande politiken vilket jag tror att EU har förstått, i och med deras initiativ de nyligen tog med att bli en ”molnaktiv” region(Rådmark, 2011c). Jag anser det vara ett välbehövligt initiativ att EU tar ställning till att vilja driva fram en tydligare molnpolitik, speciellt med tanke på oklarheterna kring de legala aspekterna.

Framtidssynen

Samtliga respondenter såg väldigt ljust på framtiden för molnet samt molntjänster. I och med användningen kommer ökas kommer molntjänster rationaliseras ytterligare som förhoppningsvis leder till klarheter gällande ovanstående utmaningar inom säkerhetsaspekter samt legala aspekter.

Förslag till fortsatt forskning

Denna studie undersökte riskerna som upplevs idag. Ju längre tiden går samt ju mer molntjänster mognar desto mer ökar kunskapen och medvetenheten. När kunskapen ökar brukar uppfattningar ändras därför vill jag föreslå fortsatt forskning kring de upplevda riskerna ett år framåt.

6. Slutsats

Syftet med studien var att undersöka de upplevda respektive faktiska riskerna med att placera tjänster och information i molnet. Frågeställningen för studien blev följaktligen:

- Vad finns det för risker med att placera tjänster och information i molnet?

De risker och osäkerheter i molnet som identifierades i empirin samt litteraturen, är högst legitima om man inte gör de förberedelser som krävs. Ansvaret ligger på en själv att säkerställa att man agerar rätt. Molnleverantörer kan ge garantier på saker och ting men ansvaret förblir på en själv.

Det visade sig att oron för riskerna gjorde att man upplevde riskerna större än de faktiskt är.

Angående oron över oklarheter i vad gäller avtal har visat sig vara en stor utmaning som kommer finnas en tid till. Avtalen i sig fokuserar mycket på vad som kan gå dåligt. Jag håller med argumentet att avtal och kontraktering skapar indirekt tillit. Skulle därför vilja föreslå att man först och främst borde ändra sättet att tänka kring avtal och kontraktering överhuvudtaget för att underlätta problematiken. Istället för att fokusera på vad som kan gå dåligt borde man istället fokusera på hur man kan göra de rätta sakerna. Detta blir möjligt anser jag genom ökad kunskap och medvetenhet samt i förlängningen ökad tillit.

Frågan är inte längre om, utan när det riktiga genombrottet för molntjänster kommer. Det har visat sig vara en lång väg kvar till dess. Även om EU startat ett initiativ för att skapa bättre förutsättningar för molnkunder gäller det ändå just nu att vara så medveten som möjligt så molnet och molntjänster får sin tid att mogna.

Först kan man tycka se endast mörka moln men genom att stegvist förbereda sig kommer man märka att molnen blir allt ljusare och ljusare.

7. Referenser

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., et al. (2009). Above the Clouds: A Berkeley View of Cloud Computing. *Computing*, (UCB/EECS-2009-28), 07-013. EECS Department, University of California, Berkeley. Hämtad från http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

Bona, A. & Ridder, F. (2011) ”IT Procurement Best Practice: Nine Contractual Terms to Reduce Risk in Cloud Contracts”, *Gartner Research*, ID Number G00211616

Blount, S. & Zanella, R. (2010) *Cloud Security and Governance, Who's on your Cloud?*. Cambridgeshire, United Kingdom: IT Governance Publishing.

Casper, C. (2011) “Privacy in the Cloud”, *Gartner Research*, ID Number G00210881.

CIO Fokus (2011) ”Molnet”, White Paper, CIO Sweden, Hämtad från http://tjanster.idg.se/globalincludes/globalservices/whitepapers/wp_document.asp?did=1367&catObjId=

Coetzee, M. & Eloff, J.H.P. (2005) ”Autonomous trust for web services”, *Internet Research*, 15(5), 498-507

Conway, G. (2011) ”Introduction to Cloud Computing”, White Paper, Innovation Value Institute, Hämtad från http://ivi.nuim.ie/publications/index.shtml#white

Cooke, J. (2011) ”IBM: ”Alla ska vinna affärsnytta i molnet”.”, *IDG: Cloud Magazine.* 4 april. http://www.idg.se/2.1085/1.377742/ibm-alla-ska-vinna-affarsnytta-i-molnet (Hämtad 2011-04-04)

European Parliament & Council Directive (EC) 1995/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Hämtad från: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Glaad, M. (2011) ”Skiftet kommer sakta men säkert.”, *IDG: Cloud Magazine.* 12 april. http://cloud.idg.se/2.16150/1.379401/skiftet-kommer-sakta-men-sakert (Hämtad 2011-05-18)

Hesier, J. & Nicolett, M. (2008) ”Assessing the Security Risks of Cloud Computing”, *Gartner Research*, ID Number G00157782.

Logan, D. (2009) “Compliance in the Cloud: Whose Data Is It Anyway?”, *Gartner Research*, ID Number G00165736

Nelson, M-R., (2009) "The Cloud, the Crowd, and Public Policy." *Issues in Science and Technology*, Summer, 71-76.

NIST (2011) ”Guidelines in Security and Privacy in Public Cloud Computing”, NIST (National Institute of Standards and Technology), Hämtad från: http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800144_cloudcomputing.pdf

Patel, R. & Davidson, B. (2003) Forskningsmetodikens grunder. *Lund, Studentlitteratur.*

Pearson, S. & Charlesworth, A. (2009) ”Accountability as a Way Forward for Privacy Protection in the Cloud”, *CloudCom 2009, LNCS 5931*, 131-144

Plummer, D-C. (2010) ”The Implications of Rights and Responsibilities ’in the cloud’”, *Gartner Research*, ID Number G000206441.

Plummer, D-C., Smith, D-M., Bittman, T-J., Cearley, D-W., Cappucio, D-J., Scott, D., Kumar, R., Robertson, B. (2009) “Five Refining Attributes of Public and Private Cloud Computing”, *Gartner Reaserch*, ID Number G00167182

Ponemon Institute (2011) ”Security of Cloud Computing Providers Study”, Research Report, Ponemon Institute, Hämtad från: http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf

Rittinghouse, J.W. & Ransome, J.F. (2010) *“Cloud Computing: Implementation, Management, and Security*”, Boca Raton, Florida: Taylor and Francis Group, LLC.

Rosengren, L. (2011) ”Microsofts vd: “Vi tror att molnet kommer växa under 2011”. ”, *CIO Sweden*. 8 mars. http://cio.idg.se/2.1782/1.372587 (Hämtad 2011-04-02)

Rådmark, H. (2011a) ”Så får du med dig ledningen i molnet”. *CIO Sweden*. 27 mars. http://cio.idg.se/2.1782/1.381356/sa-far-du-med-dig-ledningen-i-molnet (Hämtad 2011-04-02)

Rådmark, H. (2011b) ”Molnet sparar 700 miljarder under 2011”. *CIO Sweden.* 28 mars. http://cio.idg.se/2.1782/1.376609/molnet-sparar-700-miljarder-under-2011 (Hämtad 2011-05-19)

Rådmark, H. (2011c) ”EU vill ha hjälp med att driva molnet”. *CIO Sweden.* 18 maj. http://cio.idg.se/2.1782/1.386176/eu-vill-ha-hjalp-med-att-driva-molnet (Hämtad 2011-05-20)

Sangroya, A., Kumar, S., Dhok, J., Varma, V. (2010) ”Towards Analyzing Data Security Risks in Cloud Computing Environments”, *Communications in Computer and Information Science*, 54, 255-265.

Smith, D-M. (2010) ”Hype Cycle for Cloud Computing, 2010”, *Gartner Research*, ID Number G00201557

Smith, D-M. & Cearley, D-W. (2010) ”NIST and Gartner Cloud Approaches Are More Similar Than Different”, *Gartner Research*, ID Number G00173137

Svantesson, D. & Clarke, R (2010) ”Privacy and consumer risks in cloud computing”, *Computer Law & Security*, 26, 391-397.

Söderlind, M. (2011) ”Tuffa frågor till tre molnleverantörer”. ”*Tech World”*, 11 april. http://techworld.idg.se/2.2524/1.378908/tuffa-fragor-till-tre-molnleverantorer/ (Hämtad 2011-05-20)

U.S. Department of Commerce (2000) ”*U.S.-EU Safe Harbor Program”*, U.S. Department of Commerce, Hämtad från: http://www.export.gov/safeharbor/eu/eg_main_018476.asp

Zizzis, D. & Lekkas, D. (2010) ”Adressing cloud computing security issues”, *Future Generation Systems*, doi: 10.1016/j.future.2010.12.006

8. Bilagor

8.1 Intervjufrågor

Inledande frågor om respondenten och bakgrund

- Vad har du för roll/arbetsområde på Acando?
- Skulle du kunna berätta lite kortfattat om vad du har för bakgrund?

Molnet

- Hur definierar du molnet och molntjänster?
- Anser du att det är säkert att placera ut tjänster och information i molnet?
    - Om ja; Varför anser du det vara säkert? Förklara.
    - Om nej; Varför anser du det inte vara säkert? Förklara.
- Vad anser du vara den största risken med att flytta data till molnet?

Kunder

- Vad är den främsta anledningen hos era kunder för att börja använda molntjänster?
- Vad är era kunders uppfattning om molnet?
- Har någon utav era kunder uttryckt en oro över att flytta data till molnet?
    - Om ja; Vad har man då varit mest oroad över?
    - **Forts**; Hur tillmötesgår ni era kunders oro / Hur tillmötesgår ni riskerna?
- Om en potentiell ny kund kommer till er och är intresserad av molnet, vad brukar vara de vanligaste frågor ni får?
- Skulle du kunna kortfattat redogöra steg för steg hur det ser ut från att en ny kund kommer till er, till färdig implementation?
- I ett projekt med någon av era kunder, har du uppfattat något vara extra utmanande? (t.ex. aspekter inom teknik, säkerhet, avtal, risker)
    - Vad och varför har du upplevt det vara utmanande?
- Om du nu försöker att sammanfatta de ”molnprojekt” du har deltagit i hittills, vad skulle du säga vara den gemensamma nämnaren för alla dessa projekt?
    - Förtydligande; T.ex. attityder för molnet, upplevda risker,

****Tilläggsfrågor inom juridik**

- Hur förhåller ni er till EUs datalag (EU direktivet)?
- Vad är din uppfattning om molnleverantörernas avtal och de regelverk som finns?

Avslutande frågor – kompletteringar

- Hur ser du på molntjänster och dess framtid?
- Finns det något du skulle vilja tillägga som inte kommit med i frågorna men ändå är av stor betydelse?